



## **PRIVACY POLICY AT MPA RECRUITMENT**

The Company is a recruitment business which provides work-finding services to its clients and work-seekers. The Company must process personal data (including sensitive personal data) so that it can provide these services – in doing so, the Company acts as a data controller.

You may give your personal details to the Company directly, such as on an application or registration form or via our website, or we may collect them from another source such as a jobs board. The Company must have a legal basis for processing your personal data. For the purposes of providing you with work-finding services and/or information relating to roles relevant to you we will only use your personal data in accordance with this privacy statement. At all times we will comply with current data protection laws.

### **1. Collection and use of personal data**

#### **a. Purpose of processing and legal basis**

The Company will collect your personal data (which may include sensitive personal data) and will process your personal data for the purposes of providing you with work-finding services. This includes for example, contacting you about job opportunities, assessing your suitability for those opportunities, updating our databases, putting you forward for job opportunities, arranging payments to you and developing and managing our services and relationship with you and our clients.

In some cases, we may be required to use your data for the purpose of investigating, reporting and detecting crime and also to comply with laws that apply to us. We may also use your information during the course of internal audits to demonstrate our compliance with certain industry standards.

We must have a legal basis to process your personal data. The legal bases we rely upon to offer our work-finding services to you are:

- Your consent
- Where we have a legitimate interest
- To comply with a legal obligation that we have
- To fulfil a contractual obligation that we have with you

## **b. Legitimate interest**

This is where the Company has a legitimate reason to process your data provided it is reasonable and does not go against what you would reasonably expect from us. Where the Company has relied on a legitimate interest to process your personal data our legitimate interests is/are as follows:

- Managing our database and keeping work-seeker records up to date;
- Providing work-finding services to you and our clients;
- Contacting you to seek your consent where we need it;
- Giving you information about similar products or services that you have used from us recently;

## **c. Statutory/contractual requirement**

The Company has certain legal and contractual requirements to collect personal data (e.g. to comply with the Conduct of Employment Agencies and Employment Businesses Regulations 2003, immigration and tax legislation, and in some circumstances safeguarding requirements.) Our clients may also require this personal data, and/or we may need your data to enter into a contract with you. If you do not give us personal data, we need to collect we may not be able to continue to provide work-finding services to you.

## **d. Recipient/s of data**

The Company will process your personal data and/or sensitive personal data with the following recipients:

- Clients (whom we may introduce or supply you to)
- Former employers whom we may seek references from
- Payroll service providers who manage payroll on our behalf or other payment intermediaries whom we may introduce you to Other recruitment agencies in the supply chain
- Regulatory bodies (sector specific)

## **2. Overseas Transfers**

The Company may transfer the information you provide to us to countries outside the European Economic Area ('EEA') for the purposes of providing you with work-finding services. We will take steps to ensure adequate protections are in place to ensure the security of your information. The EEA comprises the EU member states plus Norway, Iceland and Liechtenstein.

## **3. Data retention**

The Company will retain your personal data only for as long as is necessary for the purpose we collect it. Different laws may also require us to keep different data for different periods of time. For example, the Conduct of Employment Agencies and Employment Businesses Regulations 2003, require us to keep work-seeker records for at least one year from (a) the date of their creation or (b) after the date on which we last provide you with work-finding services.

We must also keep your payroll records, holiday pay, sick pay and pensions auto-enrolment records for as long as is legally required by HMRC and associated national minimum wage, social security and tax legislation. This is currently 3 to 6 years.

Where the Company has obtained your consent to process your [personal [and] sensitive personal data we will do so in line with our retention policy. Upon expiry of that period the Company will seek further consent from you. Where consent is not granted the Company will cease to process your [personal data/[and] sensitive personal] data].

## **4. Your rights**

Please be aware that you have the following data protection rights:

The right to be informed about the personal data the Company processes on you;

- The right of access to the personal data the Company processes on you;
- The right to rectification of your personal data;
- The right to erasure of your personal data in certain circumstances;
- The right to restrict processing of your personal data;
- The right to data portability in certain circumstances;

- The right to object to the processing of your personal data that was based on a public or legitimate interest;
- The right not to be subjected to automated decision making and profiling; and
- The right to withdraw consent at any time.

Where you have consented to the Company processing your personal data and sensitive personal data you have the right to withdraw that consent at any time by contacting MPA's Data protection team [dataprotection@mparecruitment.co.uk](mailto:dataprotection@mparecruitment.co.uk) Please note that if you withdraw your consent to further processing that does not affect any processing done prior to the withdrawal of that consent, or which is done according to another legal basis.

There may be circumstances where the Company will still need to process your data for legal or official reasons. Where this is the case, we will tell you and we will restrict the data to only what is necessary for those specific reasons.

If you believe that any of your data that the Company processes is incorrect or incomplete, please contact us using the details above and we will take reasonable steps to check its accuracy and correct it where necessary.

You can also contact us using the above details if you want us to restrict the type or amount of data we process for you, access your personal data or exercise any of the other rights listed above.

## **5. Automated decision-making**

Recruitment processes are not based solely on automated decision-making

## **6. Log Files**

We use IP addresses to analyse trends, administer the site, track users' movements, and to gather broad demographic information for aggregate use. IP addresses are not linked to personally identifiable information.

## **7. Links to external websites**

The Company's website may contain links to other external websites. Please be aware that the Company is not responsible for the privacy practices of such other sites. When you leave our site we encourage you to read the privacy statements of each and every website that collects personally identifiable information. This privacy statement applies solely to information collected by the Company's website.

## **8. Sale of business**

If the Company's business is sold or integrated with another business your details may be disclosed to our advisers and any prospective purchasers and their advisers and will be passed on to the new owners of the business.

## **9. Data Security**

The Company takes every precaution to protect our users' information.

### **Local Access**

- Each user terminal is password protected and all logins (successful or failed) are recorded and audited regularly.
- All locations connected to the internet are protected by a business class firewall to prevent unauthorised access to user information.
- Each branch has a separate Wifi network available for public use that is isolated from all other network traffic. This prevents staff or members of the public accessing personal or corporate information.
- Personal devices are not permitted to be connected to the company network or computers.

### **Systems and User Groups**

- High risk systems that contain large quantities or personal data (i.e Sage Payroll) have unique login and password combinations for all users.
- All payroll data is encrypted on our server and logs are audited regularly.
- For all internal systems users are part of a user group that defines their level of access to stored information. This can restrict users ability to view personal information not associated with their job role.

## **Cloud Storage**

- All emails are facilitated by Microsoft Office 365 and each user has a unique randomly generated password.
- All user documents are stored on either Microsoft OneDrive or Microsoft Sharepoint and each user has a unique randomly generated password.
- All security settings are reviewed and audited regularly.

## **Website**

- Individual login details for each user with unique passwords.
- Our website is secured by SSL certification (SHA-256 bit encryption) ensuring all data transferred between a user's computer and our website server is encrypted.

Only employees who need the information to perform a specific job (for example, consultants, our accounts clerk or a marketing assistant) are granted access to your information.

The Company uses all reasonable efforts to safeguard your personal information. However, you should be aware that the use of email/ the Internet is not entirely secure and for this reason the Company cannot guarantee the security or integrity of any personal information which is transferred from you or to you via email/ the Internet.

If you share a device with others we recommend that you do not select the “remember my details” function when that option is offered.

If you have any questions about the security at our website, you can email [dataprotection@mparecruitment.co.uk](mailto:dataprotection@mparecruitment.co.uk)

## **10. Changes to this privacy statement**

We will update this privacy statement from time to time. We will post any changes on the statement with revision dates. If we make any material changes, we will notify you.

## **11. Complaints or queries**

If you wish to complain about this privacy notice or any of the procedures set out in it, please contact: MPA's Data protection Team on [dataprotection@mparecruitment.co.uk](mailto:dataprotection@mparecruitment.co.uk)

You also have the right to raise concerns with Information Commissioner's Office on 0303 123 1113 or at <https://ico.org.uk/concerns>, or any other relevant supervisory authority should your personal data be processed outside of the UK, if you believe that your data protection rights have not been adhered to.